Solution Overview: totemomail® Encryption Gateway

Around the world, there is a trend towards more stringent industry regulations and stricter compliance standards becoming apparent. This sets tougher requirements for the email security at businesses and organizations of any size and in any industry. Violating regulations such as GLBA, HIPAA, SOX, EU DPD, or Basel III or losing valuable company information can have serious consequences: financial penalties, economic damage and loss of trust on both the partner's and customer's behalf among them.

Email communication is particularly vulnerable to data loss. Whoever wants to intercept data traffic can do so without great effort. As a matter of fact, most breaches of data privacy policies can be traced back to deficient email security. But despite the obvious shortcomings of email, it has become unimaginable to stop using email in business communication.

Message confidentiality, integrity and authenticity thus need to be ensured with additional measures. Hence it is becoming increasingly important for most companies to use a reliable secure messaging solution that protects sensitive information even when on the move. FIPS 140-2-validated **totemo**mail® Encryption Gateway is optimized for mobile devices and helps strictly observe security policies as well as monitor them comprehensively for internal and external audits.

totemomail® Encryption Gateway pursues a consistent all-in-one approach for encryption. It protects confidential email communication with any given external partner. Encrypted transmission of all emails including delivery confirmation, sender identification, guaranteed message integrity as well as message non-repudiation are the automated core functionalities of the solution.

totemomail® Encryption Gateway is completely transparent, requires neither additional email clients nor plug-ins and is therefore easily and quickly integrated into any existing environment. The sender and the recipient do not need to adapt their work processes since the company security policies are centrally defined and applied.

Moreover, it is flexibly scalable and capable of multi-tenancy. If operated in a clustered environment, all settings can be configured on a single system. Furthermore, the solution is fully compatible with a number of third-party systems.

totemomail® Encryption Gateway protects your email communication with customers and business partners whereas **totemo**mail® Internal Encryption secures your internal email traffic. In combination, they become the innovative and potent hybrid encryption solution **totemo**mail® Hybrid Encryption.

How It Works

totemomail® Encryption Gateway reduces operation costs, administrative load and unintended errors to an absolute minimum through its high level of automation. The solution is easy to use and extremely secure and efficient as a result.

All electronic messages are centrally encrypted and decrypted at the company. Company security policies can be centrally defined and are automatically applied to the emails. Even the enrollment of users and communication partners takes place automatically.

Each time an email is sent to an external recipient, **totemo**mail® Encryption Gateway checks if there is a user profile for this external recipient stored in an encrypted database.

If the **software finds an entry for the recipient**, the email is encrypted, signed and sent according to the existing user profile, which also contains information on the user's preferred encryption method.

If **there is no entry for this external recipient**, an email is automatically sent to the recipient to initiate the registration process. The recipient is registered and authenticated through this process. He can also establish a preferred method for receiving encrypted messages.

The original message is retained and remains encrypted until the user is authenticated. Thus the solution ensures that sensitive information does not leave the company network unprotected.

The methods are different depending on whether or not the recipient uses a specific encryption technology.

If the **recipient uses one of the standard email encryption technologies** such as S/MIME or OpenPGP, he replies to the email with a signed message using one of his own certificates or attaches his public PGP key to the email. **totemo**mail® Encryption Gateway validates the key and stores it in the user profile. The original email is accordingly encrypted and sent to the recipient.

In case the **recipient does not use an encryption technology** of his own, **totemo**mail® Encryption offers **totemo**mail® WebMail and **totemo**mail® *Pushed*PDF as secure alternative delivery methods.

Key Facts

totemo ag
Freihofstrasse 22, CH-8700 Küsnacht, info@totemo.com, www.totemo.com, T +41 44 914 99 00, F +41 44 914 99 99

Automated Certificate and Key Management

totemomail® Encryption Gateway's core function is its automated certificate and key management. The company certificate policies can be easily and comprehensively configured using the graphical user interface of the administration console.

Among other things, you can define the settings for trustworthy certificate authorities (CA), the online validation of certificates, the required attributes for certificate and key checks as well as the validity period of certificates generated by **totemo**mail® Encryption Gateway.

By means of the automatic user enrollment feature or request to a key server, the software independently collects and encrypts the certificates and keys already available, and then saves them within the key store. **totemo**mail® Encryption Gateway's incorporated PKI component is able to generate, distribute and manage certificates for both internal and external communication partners, enabling their quick and efficient integration.

Alternatively, **totemo**mail® Encryption Gateway can be connected to an external PKI solution or CA (for example, S-Trust, Swisscom, SwissSign, QuoVadis, SignTrust etc.) via one of the numerous integrated standard interfaces.

Automated User Enrollment

totemomail® Encryption Gateway independently identifies internal and external users and enrolls them without any manual intervention by the sender or an administrator. Thus the administrative load is kept as low as possible.

For first-time recipients, **totemo**mail® Encryption Gateway retains the original message until they are successfully authenticated. Then they receive their email either digitally signed and encrypted with the matching key, via **totemo**mail® WebMail or as a **totemo**mail® *Pushed*PDF.

Administration via Graphical User Interface

totemomail® Encryption Gateway offers a web-based administration console with a graphical user interface, a dashboard and a message tracking center. No programming skills are required to define the security policies for email workflows. The administration of the whole solution can be shared between several employees.

Defining Security Policies

The company security policies as well as the corresponding email workflows are defined in the administration console. It allows a virtually infinite combination of complex rules as well as their automated application such as the encryption of any message sent to a specific domain. Along with the integrated group management, even functional mailboxes, escalation procedures, etc. can be easily configured and applied.

Comprehensive Automated Reporting

totemomail® Encryption Gateway offers comprehensive reporting capabilities. The required reports are automatically generated and delivered to the defined recipients in scheduled intervals. The reporting settings can be comfortably configured and managed in the administration console.

Enhanced Observance of Compliance Standards due to Auditability

Complete and easily searchable records of all compliance-related actions are needed for internal and external audits and reviews. **totemo**mail® Encryption Gateway caters to that need with auditable log files, a read-only role for audit users and enhanced tracking functionalities.

Benefits

Organization

- Flexible and secure email communication with external partners with or without an encryption technology of their own
- Security and cost-efficiency due to high level of automation and ease of use
- Central encryption and decryption of emails
- Central definition and application of security policies and compliance standards
- Investment protection and strategic freedom through numerous interfaces with third-party systems

Administration

- Easy integration into existing IT infrastructure
- No installation of specific email clients or plug-ins necessary – neither for employees nor business partners or customers
- Graphical user interface for administration console
- Granular definition of user roles
- No user training necessary due to transparent handling

User

- Easy and secure communication with external partners
- Work processes and software remain unaffected by implementation, no need to learn new software program
- Consistent observance of security policies and compliance standards

Architecture

totemomail® Encryption Gateway communicates directly with all current email clients. Thus neither internal users nor external communication partners need to install additional components.

The following shows the standard architecture of **totemo**mail® Encryption Gateway as part of the hybrid encryption solution.